PRIVACY IMPACT ASSESSMENT (PIA)

For the

Interoperability Layer Service (IoLS)
Defense Manpower Data Center

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☒ **New DoD Information System** ☐ **New Electronic Collection**

☐ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☐ **Yes, DITPR** Enter DITPR System Identification Number

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number

☒ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier in process

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 113, Secretary of Defense; Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08, Security of DoD Installations and Resources; DoD 5200.08-R, Physical Security Program; DoD Directive 5200.27 (Section IV A and B), Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense and E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

To evaluate individuals' eligibility for access to DoD facilities or installations and implement security standards controlling entry to DoD facilities and installations. This process includes vetting to determine the fitness of an individual requesting or requiring access, and issuance of local access credentials for members of the public requesting access to DoD facilities and installations and managing and providing updated security and credential information on these individuals. To ensure that information from DoD and other Federal agencies is considered when determining whether to grant physical access to DoD facilities and installations.

Types of information collected include: Name, date of birth, Social Security Number, Foreign National ID, Driver's License, citizenship information, gender, race, contact information, credential information, biometric information, physical features, information generated from the National Crime Information Center (NCIC).

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Access to personal information is limited to those individuals who manage the records or facilities who perform official duties. Activities must be a part of DoD government and accredited on the basis of authorized requirements. All data transfers and information retrievals that use remote communication facilities are encrypted. Electronic records are maintained in encrypted database in a controlled area accessible only to authorized personnel. Entry to these areas is restricted by the use of locks, guards, and administrative procedures.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. DoD Visitor Registration facilities

☒ **Other DoD Components.**

Specify. USA, USAF, USMC, USN

☒ **Other Federal Agencies.**

Specify. Data may be provided to other Federal agencies under any of the DoD "Blanket Routine Uses" published at http://dpclo.defense.gov/privacy/SORNs/blanket_routine_uses.html

☒ **State and Local Agencies.**

Specify. Data may be provided to state and local agencies under the DoD "Blanket Routine Uses" published at http://dpclo.defense.gov/privacy/SORNs/blanket_routine_uses.html

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

For identity data provided from DEERS and the PACS: Every registration workstation has the privacy act notification posted (responsibility of each institution) and an individual requesting access to that installation may decline to be registered - however, they will likely be rejected from receiving physical access to DoD facilities or installations.

For data provided from NCIC: Individuals do not have the opportunity to consent to the specific uses of their PII when the collection is associated with criminal and law enforcement efforts.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

For data provided from the PACS: It is the responsibility of each registration center to provide Privacy Act Statements, as required by 5 U.S.C 552a(e)(3), at the collection point. The statement should provide the following: collection purpose, authorities, external uses, the voluntary nature of the program, the fact that no consequences accrue for those who choose not to participate beyond denial of a DoD card or visitors pass and denial of access to the installation or facility, the name and number of the Privacy Act system notice governing the collection, and an electronic link to the system notice.

For identity data provided from DEERS: Privacy Act Statements are printed on DD Forms 1172, 1172-2 and 2842 and provided at the collection point. The statement provides collection purpose, authorities, external uses, nature of the program, the name and number of the PAS notice governing the collection, and an electronic link to the system notice. The statement is included on paper and electronic collection forms. A PAS is also available for those updating their information via telephone.

For data provided from the NCIC: None.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☒ **Other** ☒ **None**

Describe each applicable format.

For data provided from the PACS It is the responsibility of each registration center to provide Privacy Act Statements, as required by 5 U.S.C 552a(e)(3), at the collection point. The statement should provide the following: collection purpose, authorities, external uses, the voluntary nature of the program, the fact that no consequences accrue for those who choose not to participate beyond denial of a DoD card or visitors pass and denial of access to the installation or facility, the name and number of the Privacy Act system notice governing the collection, and an electronic link to the system notice.

For identity data provided from DEERS: Privacy Act Statements are printed on DD Forms 1172, 1172-2 and 2842 and provided at the collection point. The statement provides collection purpose, authorities, external uses, nature of the program, the name and number of the PAS notice governing the collection, and an electronic link to the system notice. The statement is included on paper and electronic collection forms. A PAS is also available for those updating their information via telephone.

For data provided from the NCIC: None.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.